Scott Edward Cole, Esq. (S.B. #160744)
Laura Grace Van Note, Esq. (S.B. #310160)
Cody Alexander Bolce, Esq. (S.B. #322725)
SCOTT COLE & ASSOCIATES, APC
555 12th Street, Suite 1725
Oakland, California 94607
Telephone: (510) 891-9800
Facsimile: (510) 891-7030
Email: scole@scalaw.com
Email: lvannote@scalaw.com
Email: cbolce@scalaw.com
Web: www.scalaw.com

Attorneys for Representative Plaintiff and the Plaintiff Classes

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

ANGELICA MENDOZA, individually, and on behalf of all others similarly situated,

Plaintiffs,

vs.

NEC NETWORKS, LLC d/b/a CAPTURERX, RITE AID CORPORATION, COMMUNITY HEALTH CENTERS OF THE CENTRAL COAST, INC.,

Defendants.

Case No.

CLASS ACTION

PLAINTIFFS' COMPLAINT FOR DAMAGES, INJUNCTIVE AND EQUITABLE RELIEF FOR:

1. **NEGLIGENCE;**
2. **INVASION OF PRIVACY;**
3. **BREACH OF CONFIDENCE;**
4. **INFORMATION PRACTICES ACT OF 1977 (CAL. CIV. CODE §1798);**
5. **CONFIDENTIALITY OF MEDICAL INFORMATION ACT (CAL. CIV. CODE §56);**
6. **BREACH OF IMPLIED CONTRACT;**
7. **BREACH OF THE IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING;**
8. **UNFAIR BUSINESS PRACTICES;**
9. **UNJUST ENRICHMENT**

JURY TRIAL DEMANDED

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

Representative Plaintiff alleges as follows:

INTRODUCTION

1. Representative Plaintiff bring this class action against Defendants NEC Networks, LLC, d/b/a CaptureRx, Rite Aid Corporation and Community Health Centers of the Central Coast, Inc. (collectively "Defendants") for their respective failures to properly secure and safeguard Representative Plaintiff's and Class Members' personally identifiable information stored within Defendants' information networks, including, without limitation, their names, dates of birth, and prescription information (these types of information, *inter alia*, being hereafter referred to, collectively, as "personally identifiable information" or "PII")[1] and to properly secure and safeguard Representative Plaintiff's and Class Members' personal health information ("PHI")[2] stored within Defendants' information network.

2. With this action, Representative Plaintiff seek to hold Defendant CaptureRx responsible for the harms it caused Representative Plaintiff and the 1.6 to 2.4 million other similarly situated persons in the massive and preventable cyber-attack that took place starting on or around February 6, 2021, by which cybercriminals infiltrated Defendants' inadequately protected network servers where highly sensitive PII/PHI was being kept unprotected (the "2021 Data Breach").[3]

3. Representative Plaintiff further seeks to hold Defendants Rite Aid Corporation and Community Health Centers of the Central Coast, Inc. responsible for entrusting this highly

---

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on their face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers).

[2] Personal health information ("PHI") is a category of information that refers to an individual's medical records and history, which is protected under the Health Insurance Portability and Accountability Act (HIPAA). Inter alia, PHI includes test results, procedure descriptions, diagnoses, personal or family medical histories and data points applied to a set of demographic information for a particular patient.

[3] *See,* https://www.capturerx.com/data-incident/ (last accessed August 8, 2021).

sensitive PII/PHI Defendants CaptureRx, not ensuring that Defendants CaptureRx maintained the PII/PHI in a manner consistent with industry, the Health Insurance Portability and Accountability Act of 1996 ("HIPPA") Privacy Rule (45 CFR, Parts 160 and 164(A) and (E)), the HIPPA Security Rule (45 CFR, Parts 160 and 164(A) and (C)), and other relevant standards.

4. When CaptureRx reported the security incident to the Department of Health and Human Services Office for Civil Rights on May 5, 2021, CaptureRx alleged the 2021 Data Breach affected nearly 1.7 million individuals. As of a July 12, 2021 updated breach notification, CaptureRx indicated that the Data Breach victim tally had grown to more than 2.4 million individuals.[4]

5. On its website, as of August 8, 2021, CaptureRx lists nearly 150 affected healthcare providers to whom it issued its 2021 Data Breach notice.[5]

6. Through the use of malware, unauthorized persons infiltrated Defendants' network servers which housed its members' sensitive PII that included names, dates of birth, and prescription information.

7. Defendants acquired, collected and stored Representative Plaintiff's and Class Members' PII/PHI in order to ensure efficient and quality healthcare and/or pharmacy services to Representative Plaintiff and Class Members. Therefore, at all relevant times, Defendants knew or should have known that Representative Plaintiff and Class Members would use Defendants' networks to store and/or share sensitive data, including highly confidential PII/PHI, because Defendants promised them that creating personal healthcare records would improve care quality.

8. HIPAA establishes national minimum standards for the protection of individuals' medical records and other personal health information. HIPAA, generally, applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically, and sets minimum standards for Defendants' maintenance of Representative Plaintiff's and Class Members' PII/PHI. More specifically, HIPAA requires

[4] *See,* https://www.healthcareinfosecurity.com/lawsuits-against-capturerx-pile-up-so-do-victim-counts-a-17143 (last accessed August 8, 2021).

[5] *See,* https://www.capturerx.com/data-incident-provider-list/ (last accessed August 8, 2021).

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

appropriate safeguards be maintained by healthcare providers such as Defendants to protect the privacy of personal health information and sets limits and conditions on the uses and disclosures that may be made of such information without customer/patient authorization. HIPAA also establishes a series of rights over Representative Plaintiff's and Class Members' PII/PHI, including rights to examine and obtain copies of their health records, and to request corrections thereto.

9. Additionally, the HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The HIPAA Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

10. By obtaining, collecting, using, and deriving a benefit from Representative Plaintiff's and Class Members' PII/PHI, Defendants assumed legal and equitable duties to those individuals. These duties arise from HIPAA and other state and federal statutes and regulations as well as common law principles.

11. Defendants disregarded the rights of Representative Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Representative Plaintiff's and Class Members' PII/PHI was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the PII/PHI of Representative Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party—an undoubtedly nefarious third party that seeks to profit off this disclosure by defrauding Representative Plaintiff and Class Members in the future. Representative Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they are entitled to injunctive and other equitable relief.

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

JURISDICTION AND VENUE

12. Jurisdiction is proper in this Court under 28 U.S.C. §1332(d) because this is a class action where the amount in controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from one or more Defendants as Defendants serves customers/patients who are citizens of numerous states who seek medical and/or prescription service and from whom Defendants have collected and shared PII/PHI.

13. Defendants routinely conduct business in California, have sufficient minimum contacts in California and have intentionally availed themselves of this jurisdiction by marketing and selling products and services, and by accepting and processing payments for those products and services within California. Venue is, thus, proper in this Court under 28 U.S.C. § 1391 because the events that gave rise to Representative Plaintiff's and many Class Members' claims took place within the Northern District of California, Oakland Division and Defendants do business in this Judicial District.

PLAINTIFFS

14. Representative Plaintiff Angelica Mendoza ("Mendoza" and/or "Representative Plaintiff") is an adult individual and, at all relevant times herein, a resident of the State of California. Mendoza is a victim of the 2021 Data Breach.

15. Mendoza received medical services from CHC.

16. Mendoza was a consumer for purposes of obtaining prescriptions of Rite Aid.

17. At all times herein relevant, Mendoza is and was a member of the National class and the California Subclass.

18. As required in order to obtain medical and/or prescription services from Defendants, Mendoza provided Defendants with highly sensitive personal, financial, health and insurance information.

19. Mendoza's PII/PHI was exposed in the 2021 Data Breach because Defendants stored and/or shared Mendoza's PII/PHI. Her PII/PHI was within the possession and control of Defendants at the time of the 2021 Data Breach.

20. Mendoza received two letters from CaptureRx, dated May 5, 2021, informing her that her PII/PHI was involved in the 2021 Data Breach (the "Notices"). These Notices explained that CaptureRx became aware of unusual activity involving certain of its electronic files, investigated the activity and, as early as February 19, 2021, determined that certain files containing the PII/PHI of Class Members were accessed and unlawfully acquired (as early as February 6, 2021). What's more, according to these Notices, CaptureRx confirmed, as early as March 19, 2021, that some of Plaintiff's PII/PHI was also present in the accessed and unlawfully acquired files. Again, while, CaptureRx claims to have known of this breach and its impact on Plaintiff, and while it started notifying some Rite Aid and CHC clients as early as March 30, 2021 of the Data Breach, it did not inform Plaintiff of it until at least May 5, 2021.

21. As a result, Mendoza spent time dealing with the consequences of the 2021 Data Breach, which included and continues to include time spent on the telephone, verifying the legitimacy and impact of the 2021 Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

22. Mendoza suffered actual injury in the form of damages to and diminution in the value of her PII/PHI—a form of intangible property that she entrusted to Defendants for the purpose of obtaining her prescription medication, which was compromised in and as a result of the 2021 Data Breach.

23. Mendoza suffered lost time, annoyance, interference, and inconvenience as a result of the 2021 Data Breach and has anxiety and increased concerns for the loss of her privacy, as well as anxiety over possibly losing access to her necessary prescription medications.

24. Mendoza has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII/PHI, in

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

combination with her name, being placed in the hands of unauthorized third-parties and possibly criminals.

25. Mendoza has a continuing interest in ensuring that her PII/PHI, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

DEFENDANTS

26. NEC Networks, LLC, d/b/a CaptureRx ("CaptureRx"), is a Texas limited liability company with its principle place of business in San Antonio, Texas. CaptureRx is a specialty pharmacy benefits manager. Its services include prescription claims processing, patient assistance program administration and public health service 340B drug program administration. CaptureRx provides these services for pharmacies and healthcare providers across the United States, including the remaining defendants identified herein. To carry out those services, CaptureRx collected, stored and shared the PII/PHI of Representative Plaintiff and all Class Members.

27. Rite Aid Corporation ("Rite Aid") is an American drugstore chain headquartered in Camp Hill, Pennsylvania. Rite Aid is the largest drugstore chain on the East Coast and the third largest drugstore chain in the nation. Rite Aid provided prescription services to Representative Plaintiff and numerous Class Members. To carry out those services, Rite Aid collected, stored and shared the PII/PHI of Representative Plaintiff and numerous Class Members.

28. Defendants Community Health Centers of the Central Coast, Inc. ("CHC") is a California 501(c)(3) non-profit network of community health centers serving the residents of California's Central Coast. CHC's 26 licensed primary medical and dental care clinic network provides urgent health care services, including health screening and assessment, dental screening, health education, on-site medical treatment and/or referral, and transportation to medical treatment. CHC provided medical services to Representative Plaintiff and numerous Class Members. To carry out those services, Rite Aid collected, stored and shared the PII/PHI of Representative Plaintiff and numerous Class Members.

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

29. Defendants Rite Aid and CHC contracted with Defendants CaptureRx to process claims and/or otherwise facilitate Rite Aid's and CHC's pharmacy and heath care services businesses. The electronic files stored and/or shared by Defendants contained non-redacted and non-encrypted PII and PHI belonging to Representative Plaintiff and Class Members. This sensitive and confidential PII, including, but not limited to, full names and birthdates, is static and does not change, and can be used to commit myriad identity crimes. The PHI involved—identifying and prescription information—is also sensitive and confidential, and is protected, private medical treatment information that divulges not only the types of pharmaceuticals Representative Plaintiff and Class Members were prescribed, but also the underlying mental or physical diagnoses.

30. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged here are currently unknown to Representative Plaintiff. Representative Plaintiff will seek leave of Court to amend this Complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

CLASS ACTION ALLEGATIONS

31. Representative Plaintiff brings this action pursuant to the provisions of Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, on behalf of herself and the following classes/subclass(es) (collectively, the "Classes"):

> California class:
> "All individuals within the State of California whose PII/PHI was stored by Defendants and/or was exposed to unauthorized third parties as a result of the 2021 Data Breach."
>
> National class:
> "All individuals within the United States of America whose PII/PHI was stored by Defendants and/or was exposed to unauthorized third parties as a result of the 2021 Data Breach."

32. Excluded from the Classes are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants has a controlling interest; all individuals who make a timely election to be excluded

from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to its departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

33. Also, in the alternative, Representative Plaintiff requests additional Subclasses be added, as necessary, based on the types of PII/PHI that were compromised.

34. Representative Plaintiff reserves the right to amend the above definition or to propose subclasses in subsequent pleadings and/or motions for class certification.

35. This action has been brought and may properly be maintained as a class action under Federal Rule of Civil Procedure Rule 23 because there is a well-defined community of interest in the litigation and membership in the proposed classes is easily ascertainable.

a. Numerosity: A class action is the only available method for the fair and efficient adjudication of this controversy. The members of the Plaintiff Classes are so numerous that joinder of all members is impractical, if not impossible. Representative Plaintiff is informed and believes and, on that basis, alleges that the total number of Class Members is in the millions of individuals. Membership in the classes will be determined by analysis of Defendants' records.

b. Commonality: The Representative Plaintiff and the Class Members share a community of interests in that there are numerous common questions and issues of fact and law which predominate over any questions and issues solely affecting individual members, including, but not necessarily limited to:

1) Whether Defendants engaged in the wrongful conduct alleged herein;

2) Whether Defendants had a legal duty to Representative Plaintiff and the Classes to exercise due care in collecting, storing, using and/or safeguarding their PII/PHI;

3) Whether Defendants knew or should have known of the susceptibility of CaptureRx's data security systems to a data breach;

4) Whether Defendant CaptureRx's security procedures and practices to protect its systems were reasonable in light of the measures recommended by data security experts;

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

5) Whether Defendants' failure to implement adequate data security measures, including the sharing of Representative Plaintiff's and Class Members' PII/PHI allowed the 2021 Data Breach to occur and/or worsened its effects;

6) Whether Defendants failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

7) Whether Defendants adequately, promptly, and accurately informed Representative Plaintiff and Class Members that their PII/PHI had been compromised;

8) How and when Defendants actually learned of the 2021 Data Breach;

9) Whether Defendants failed to adequately respond to the 2021 Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to the Representative Plaintiff and Class Members;

10) Whether Defendants' conduct, including their failure to act, resulted in or was the proximate cause of the breach of these systems, resulting in the loss of the PII/PHI of Representative Plaintiff and Class Members;

11) Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the 2021 Data Breach to occur;

12) Whether Defendants' conduct, including their failure to act, resulted in or was the proximate cause of the 2021 Data Breach and/or damages flowing therefrom;

13) Whether Defendants' actions alleged herein constitute gross negligence and whether the negligence of any one defendant can be imputed to another;

14) Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII/PHI of Representative Plaintiff and Class Members;

15) Whether Representative Plaintiff and Class Members are entitled to actual and/or statutory damages and/or whether injunctive, corrective and/or declaratory relief and/or an accounting is/are appropriate as a result of Defendants' wrongful conduct and, if so, what is necessary

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

to redress the imminent and currently ongoing harm faced by Representative Plaintiff, Class Members and the general public;

16) Whether Representative Plaintiff and Class Members are entitled to restitution as a result of Defendants' wrongful conduct;

17) Whether Defendants continue to breach duties to Representative Plaintiff and Class Members.

c. Typicality: The Representative Plaintiff's claims are typical of the claims of the Plaintiff Classes. Representative Plaintiff and all members of the Plaintiff Classes sustained damages arising out of and caused by Defendants' common course of conduct in violation of law, as alleged herein. The same event and conduct that gave rise to Representative Plaintiff's claims are identical to those that give rise to the claims of every Class Member because Representative Plaintiff and each Class Member had their sensitive PII/PHI compromised in the same way by the same conduct of Defendants. Representative Plaintiff and all Class Members face the identical threats resulting from the breach of their PII/PHI without the protection of encryption and adequate monitoring of user behavior and activity necessary to identity those threats.

d. Adequacy of Representation: The Representative Plaintiff in this class action is an adequate representative of each of the Plaintiff Classes in that the Representative Plaintiff has the same interest in the litigation of this case as the remaining Class Members, is committed to vigorous prosecution of this case and has retained competent counsel who are experienced in conducting litigation of this nature. Representative Plaintiff is not subject to any individual defenses unique from those conceivably applicable to other Class Members or the classes in their entirety. The Representative Plaintiff anticipates no management difficulties in this litigation. Representative Plaintiff and her counsel will fairly and adequately protect the interests of all Class Members.

e. Superiority of Class Action: The damages suffered by individual Class Members, are significant, but may be small relative to the enormous expense of individual litigation by each member. This makes or may make it impractical for members of the Plaintiff Classes to seek redress individually for the wrongful conduct alleged herein. Even if Class Members could afford such individual litigation, the court system could not. Should separate actions be brought or be required to be brought, by each individual member of the Plaintiff classes, the resulting multiplicity of lawsuits would cause undue hardship and expense for the Court and the litigants. The prosecution of separate actions would also create a risk of inconsistent rulings which might be dispositive of the interests of other

Class Members who are not parties to the adjudications and/or may substantially impede their ability to adequately protect their interests. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

36. Class certification is proper because the questions raised by this Complaint are of common or general interest affecting numerous persons, such that it is impracticable to bring all Class Members before the Court.

37. This class action is also appropriate for certification because Defendants has acted or refused to act on grounds generally applicable to the Classes, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Classes in their entireties. Defendants' policies challenged herein apply to and affect Class Members uniformly and Representative Plaintiff's challenge of these policies hinges on Defendants' conduct with respect to the Classes in their entireties, not on facts or law applicable only to the Representative Plaintiff.

38. Unless a Class-wide injunction is issued, Defendants may continue in their failure to properly secure the PII/PHI of Class Members, Defendants may continue to act unlawfully as set forth in this Complaint.

COMMON FACTUAL ALLEGATIONS

The Cyber Attack

39. On or about February 6, 2021, CaptureRx servers were subject to a cyber-attack through which unauthorized third-party cybercriminals gained access to Representative Plaintiff's and Class Members' PII/PHI.

40. On or around February 19, 2021, CaptureRx began identifying unusual network activity affecting some of its information systems.

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

41. After becoming aware of this, CaptureRx alleges to have investigated the unusual network activity, an investigation which determined, as early as March 19, 2021, that unauthorized person(s) accessed CaptureRx's network and acquired Representative Plaintiff's and Class Members' PII/PHI housed on CaptureRx's network (aka, the 2021 Data Breach).

42. On or about March 30, 2021, CaptureRx started notifying Rite Aid's and CHC's (among other) clients of the incident, but did not inform Representative Plaintiff until at least May 5, 2021.

43. Representative Plaintiff was provided the information detailed above upon her receipt of two letters from CaptureRx , dated May 5, 2021. She was not aware of the 2021 Data Breach until receiving those letters.

Defendants' Failed Response to the Breach

44. On March 30, 2021, Defendants (individually and/or through CaptureRx) began mailing letters ("the Notice") to more than 1,656,569 persons whose PII/PHI Defendants could confirm was compromised as a result of the 2021 Data Breach. The letter explained details of the 2021 Data Breach and Defendants' recommended next steps such as reviewing statements received from healthcare providers and insurers.

45. The Notice included, *inter alia*, the following:

> CaptureRx is a vendor that provides services to certain healthcare providers, including Midtown Health Center, Inc. CaptureRx is writing, on behalf of Midtown Health Center, Inc. to notify you of a recent event at CaptureRx that may affect the privacy of some of your personal information. …
>
> **What Happened?**
> CaptureRx recently became aware of unusual activity involving certain of its electronic files. Following this, CaptureRx immediately began an investigation into this activity and worked quickly to assess the security of its system. On February 19, 2021, the investigation determined that certain files were accessed and acquired on February 6, 2021 without authorization. CaptureRx immediately began a thorough review of the full contents of the files to determine whether sensitive information was present at the time of the incident. On or around March 19, 2021, CaptureRx confirmed that some

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

> of your information was present in the relevant files. CaptureRx began the process of notifying Midtown on or around March 30, 2021 of this incident.
>
> **What Information Was Involved?**
> The investigation determined that, at the time of the incident, the relevant files contained your first name, last name, date of birth, and prescription information. We are providing you this notice to ensure you are aware of this incident.[6]

46. Defendants sent a sample notice of data breach letter that mirrored the language of the Notice sent to Representative Plaintiff and Class Members the California Attorney General's Office.

47. Upon information and belief, the unauthorized third-party cybercriminals gained access to Representative Plaintiff's and Class Members' PII/PHI with the intent of engaging in misuse of the PII/PHI, including marketing and selling Representative Plaintiff's and Class Members' PII/PHI.

48. Defendants had and continue to have obligations created by HIPAA, the California Confidentiality of Medical Information Act ("CMIA"), reasonable industry standards, common law, state statutory law, and their own assurances and representations to keep Representative Plaintiff's and Class Members' PII/PHI confidential and to protect such PII/PHI from unauthorized access.

49. Representative Plaintiff and Class Members were required to provide their PII/PHI to Defendants with the reasonable expectation and mutual understanding that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access.

50. Despite this, Representative Plaintiff and the Class Members remain, even today, in the dark regarding what particular data was stolen, the particular malware used, and what steps are being taken, if any, to secure their PII/PHI going forward. Especially in light of CaptureRx's suggestion that individuals require "guidance on how to protect against identity theft and

[6] *See, e.g.,* https://agportal-s3bucket.s3.amazonaws.com/Data_Breach/NECNetworks DbaCaptureRx.2021-05-05.pdf

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

fraud…information on how to place a fraud alert and security freeze on one's credit file…,"[7] Representative Plaintiff and Class Members are left to speculate as to the full impact of the 2021 Data Breach and how exactly Defendants intend to enhance their information security systems and monitoring capabilities so as to prevent further breaches.

51. Representative Plaintiff's and Class Members' PII/PHI may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII/PHI for targeted marketing without the approval of Representative Plaintiff and/or Class Members. Either way, unauthorized individuals can now easily access the PII/PHI of Representative Plaintiff and Class Members.

Defendants Collected and Stored Representative Plaintiff's and Class Members' PII/PHI

52. Defendants acquired, collected, and stored and assured reasonable security over Representative Plaintiff's and Class Members' PII/PHI.

53. As a condition of their relationships with Representative Plaintiff and Class Members, Defendants required that Representative Plaintiff and Class Members entrust Defendants with highly sensitive and confidential PII and PHI.

54. By obtaining, collecting, and storing Representative Plaintiff's and Class Members' PII, Defendants assumed legal and equitable duties and knew or should have known that they were thereafter responsible for protecting Representative Plaintiff's and Class Members' PII/PHI from unauthorized disclosure.

55. Representative Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII/PHI. Representative Plaintiff and Class Members relied on Defendants to keep their PII/PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

56. Defendants could have prevented the 2021 Data Breach by properly securing and encrypting Representative Plaintiff's and Class Members' PII/PHI.

[7] Id.

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

57. Defendants' negligence in safeguarding Representative Plaintiff's and Class Members' PII/PHI is exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years.

58. The healthcare industry has experienced a large number of high-profile cyber-attacks even in just the one-year period preceding the filing of this Complaint and cyber-attacks, generally, have become increasingly more common. More healthcare data breaches were reported in 2020 than in any other year, showing a 25% increase.[8] Additionally, according to the HIPAA Journal, the largest healthcare data breaches have been reported in April 2021.[9]

59. For example, Universal Health Services experienced a cyber-attack on September 29, 2020 that was very similar to the attack on CaptureRx. As a result, Universal Health Services suffered a four-week outage of its systems which caused as much as $67 million in recovery costs and lost revenue.[10] Similarly, in 2021, Scripps Health suffered a cyber-attack, an event which effectively shut down critical health care services for a month and leaving numerous patients unable to speak to their physicians or access vital medical and prescription records. Due to the high-profile nature of these breaches, and other breaches of their kind, Defendants were and/or certainly should have been on notice and aware of such attacks occurring in the healthcare industry and, therefore, should have assumed and adequately performed the duty of preparing for such an imminent attack.

60. Despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect Representative Plaintiff's and Class Members' PII/PHI from being compromised.

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

[8] https://www.hipaajournal.com/2020-healthcare-data-breach-report-us/ (last accessed July 28, 2021).
[9] https://www.hipaajournal.com/april-2021-healthcare-data-breach-report/ (last accessed July 28, 2021).
[10] https://ir.uhsinc.com/news-releases/news-release-details/universal-health-services-inc-reports-2020-fourth-quarter-and (last accessed July 28, 2021).

Defendants Had an Obligation to Protect the Stolen PII/PHI

61. Defendants are covered by HIPAA's Applicability (45 C.F.R. § 160.102). As such, they are required to comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

62. HIPAA's Privacy Rule or Standards for Privacy of Individually Identifiable Health Information establishes national standards for the protection of health information.

63. HIPAA's Privacy Rule or Security Standards for the Protection of Electronic Protected Health Information establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

64. HIPAA requires Defendants to "comply with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

65. "Electronic protected health information" is "individually identifiable health information … that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

66. HIPAA's Security Rule requires Defendants to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by their workforce.

67. HIPAA also requires Defendants to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

electronic protected health information." 45 C.F.R. § 164.306(e), and to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

68. Moreover, the HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414 requires Defendants to provide notice of the 2021 Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."

69. Defendants was also prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. See, e.g., *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

70. In addition to their obligations under federal and state laws, Defendants owed a duty to Representative Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII/PHI in Defendants' possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendants owed a duty to Representative Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that their computer systems, networks, and protocols adequately protected the PII/PHI of Representative Plaintiff and Class Members.

71. Defendants owed a duty to Representative Plaintiff and Class Members to design, maintain, and test their computer systems and networks to ensure that the PII/PHI in their possession was adequately secured and protected.

72. Defendants owed a duty to Representative Plaintiff and Class Members to create and implement reasonable data security practices and procedures to protect the PII/PHI in their possession, including not sharing information with other entities who maintained sub-standard data security systems.

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

73. Defendants owed a duty to Representative Plaintiff and Class Members to implement processes that would detect a breach on their data security systems in a timely manner.

74. Defendants owed a duty to Representative Plaintiff and Class Members to act upon data security warnings and alerts in a timely fashion.

75. Defendants owed a duty to Representative Plaintiff and the Classes to disclose if their computer systems and data security practices were inadequate to safeguard individuals' PII/PHI from theft because such an inadequacy would be a material fact in the decision to entrust this PII/PHI to Defendants.

76. Defendants owed a duty of care to Representative Plaintiff and the Classes because they were foreseeable and probable victims of any inadequate data security practices.

77. Defendants owed a duty to Representative Plaintiff and the Classes to encrypt Representative Plaintiff's and Class Members' PII/PHI and monitor user behavior and activity in order to identity possible threats.

Value of PII/PHI

78. The PII/PHI data accessed in such an attack represents a major score for cybercriminals. This information is of great value to them and the data stolen in the 2021 Data Breach will undoubtedly be used in a variety of sordid ways for criminals to exploit Representative Plaintiff and Class Members and to profit off their misfortune.

79. PII/PHI is a valuable commodity for which a "cyber black market" exists in which criminals openly post stolen payment card numbers, social security numbers, and other personal information on a number of underground Internet websites.

80. The high value of PII/PHI to criminals is further evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[11] Experian reports that a stolen credit or debit card

[11] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed July 28, 2021).

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

number can sell for $5 to $110 on the dark web.[12] Criminals can also purchase access to entire company data breaches from $999 to $4,995.[13]

81. Between 2005 and 2019, at least 249 million people were affected by health care data breaches.[14] Indeed, during 2019 alone, over 41 million healthcare records were exposed, stolen, or unlawfully disclosed in 505 data breaches.[15] In short, these sorts of data breaches are increasingly common, especially among healthcare systems, which account for 30.03% of overall health data breaches, according to cybersecurity firm Tenable.[16]

82. These criminal activities have and will result in devastating financial and personal losses to Representative Plaintiff and Class Members. For example, it is believed that certain PII/PHI compromised in the 2017 Experian data breach was being used, three years later, by identity thieves to apply for COVID-19-related benefits in the state of Oklahoma. Such fraud will be an omnipresent threat for Representative Plaintiff and Class Members for the rest of their lives. They will need to remain constantly vigilant.

83. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."

84. Identity thieves can use PII/PHI, such as that of Representative Plaintiff and Class Members which Defendants failed to keep secure, to perpetrate a variety of crimes that harm

[12] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed July 28, 2021).

[13] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed July 28, 2021).

[14] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133. (last accessed July 28, 2021).

[15] https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/. (last accessed July 28, 2021).

[16] https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches. (last accessed July 28, 2021).

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

victims. For instance, identity thieves may commit various types of government fraud such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits, or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

85. The ramifications of Defendants' failure to keep secure Representative Plaintiff's and Class Members' PII/PHI are long lasting and severe. Once PII/PHI is stolen, particularly identification numbers, fraudulent use of that information and damage to victims may continue for years. Indeed, the PII/PHI of Representative Plaintiff and Class Members was taken by hackers to engage in identity theft or to sell it to other criminals who will purchase the PII/PHI for that purpose. The fraudulent activity resulting from the 2021 Data Breach may not come to light for years.

86. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII/PHI is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[17]

87. The harm to Representative Plaintiff and Class Members is especially acute given the nature of the leaked data. Medical identity theft is one of the most common, most expensive, and most difficult-to-prevent forms of identity theft. According to Kaiser Health News, "medical-related identity theft accounted for 43 percent of all identity thefts reported in the United States in 2013," which is more than identity thefts involving banking and finance, the government and the military, or education.[18]

88. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy

[17] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* http://www.gao.gov/new.items/d07737.pdf (last accessed July 28, 2021).

[18] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/. (last accessed July 28, 2021).

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[19]

89. If cyber criminals manage to access financial information, health insurance information and other personally sensitive data—as they did here—there is no limit to the amount of fraud to which Defendants may expose the Representative Plaintiff and Class Members.

90. A study by Experian found that the average total cost of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[20] Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third saw their insurance premiums rise, and forty percent were never able to resolve their identity theft at all.[21]

91. And data breaches are preventable.[22] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[23] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[24]

92. Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures … Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[25]

---

[19] *Id.*
[20] See Elinor Mills, "Study: Medical Identity Theft is Costly for Victims," CNET (Mar, 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/.
[21] Id.; see also Healthcare Data Breach: What to Know About them and What to Do After One, EXPERIAN, https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/. (last accessed July 28, 2021).
[22] Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012)
[23] *Id.* at 17.
[24] *Id.* at 28.
[25] *Id.*

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

93. Here, Defendants knew of the importance of safeguarding PII/PHI and of the foreseeable consequences that would occur if Plaintiff's and Class Members' PII/PHI was stolen, including the significant costs that would be placed on Plaintiff and Class Members as a result of a breach of this magnitude. As detailed above, Defendants are large, sophisticated organizations with the resources to deploy robust cybersecurity protocols. They knew, or should have known, that the development and use of such protocols were necessary to fulfill their statutory and common law duties to Representative Plaintiff, Class Members. Their failure to do so is, therefore, intentional, willful, reckless and/or grossly negligent.

94. Defendants disregarded the rights of Representative Plaintiff and Class Members by, *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that they network servers were protected against unauthorized intrusions; (ii) failing to disclose that they did not have adequately robust security protocols and training practices in place to adequately safeguard Representative Plaintiff's and Class Members' PII/PHI; (iii) failing to take standard and reasonably available steps to prevent the 2021 Data Breach; (iv) concealing the existence and extent of the 2021 Data Breach for an unreasonable duration of time; and (v) failing to provide Representative Plaintiff and Class Members prompt and accurate notice of the 2021 Data Breach.

FIRST CLAIM FOR RELIEF
Negligence
(Both Classes)

95. Each and every allegation of the preceding paragraphs is incorporated in this cause of action with the same force and effect as though fully set forth herein.

96. At all times herein relevant, Defendants owed Representative Plaintiff and Class Members a duty of care, *inter alia*, to act with reasonable care to secure and safeguard their PII/PHI and to use commercially reasonable methods to do so. Defendants took on this obligation upon accepting and storing the PII/PHI of Representative Plaintiff and Class Members in their computer systems and on their networks.

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

97. Among these duties, Defendants were expected:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the PII/PHI in their possession;

b. to protect Representative Plaintiff's and Class Members' PII/PHI using reasonable and adequate security procedures and systems that were/are compliant with industry-standard practices;

c. to implement processes to quickly detect the 2021 Data Breach and to timely act on warnings about data breaches; and

d. to promptly notify Representative Plaintiff and Class Members of any data breach, security incident, or intrusion that affected or may have affected their PII/PHI.

98. Defendants knew that the PII/PHI was private and confidential and should be protected as private and confidential and, thus, Defendants owed a duty of care not to subject Representative Plaintiff and Class Members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

99. Defendants knew, or should have known, of the risks inherent in collecting and storing PII/PHI, the vulnerabilities of their data security systems, and the importance of adequate security. Defendants knew about numerous, well-publicized data breaches.

100. Defendants knew, or should have known, that their data systems and networks did not adequately safeguard Representative Plaintiff's and Class Members' PII/PHI.

101. Only Defendants were in the position to ensure that their systems and protocols were sufficient to protect the PII/PHI that Representative Plaintiff and Class Members had entrusted to it.

102. Defendants breached their duties to Representative Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the PII/PHI of Representative Plaintiff and Class Members.

103. Because Defendants knew that a breach of their systems could damage millions of individuals, including Representative Plaintiff and Class Members, Defendants had a duty to adequately protect their data systems and the PII/PHI contained thereon.

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

104. Representative Plaintiff's and Class Members' willingness to entrust Defendants with their PII/PHI was predicated on the understanding that Defendants would take adequate security precautions. Moreover, only Defendants had the ability to protect their systems and the PII/PHI they stored on them from attack. Thus, Defendants had a special relationship with Representative Plaintiff and Class Members.

105. Defendants also had independent duties under state and federal laws that required Defendants to reasonably safeguard Representative Plaintiff's and Class Members' PII/PHI and promptly notify them promptly about the 2021 Data Breach. These "independent duties" are untethered to any contract between Defendants and the Representative Plaintiff and/or the remaining Class Members.

106. Defendants breached their general duty of care to Representative Plaintiff and Class Members in, but not necessarily limited to, the following ways:

a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the PII/PHI of Representative Plaintiff and Class Members;

b. by failing to timely and accurately disclose that Representative Plaintiff's and Class Members' PII/PHI had been improperly acquired or accessed;

c. by failing to adequately protect and safeguard the PII/PHI by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PII/PHI;

d. by failing to provide adequate supervision and oversight of the PII/PHI with which they were and are entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather PII/PHI of Representative Plaintiff and Class Members, misuse the PII/PHI and intentionally disclose it to others without consent.

e. by failing to adequately train their employees to not store PII/PHI longer than absolutely necessary;

f. by failing to consistently enforce security policies aimed at protecting Representative Plaintiff's and the Class Members' PII/PHI;

g. by failing to implement processes to quickly detect data breaches, security incidents, or intrusions; and

h. by failing to encrypt Representative Plaintiff's and Class Members' PII/PHI and monitor user behavior and activity in order to identify possible threats.

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

107. Defendants' willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

108. As a proximate and foreseeable result of Defendants' grossly negligent conduct, Representative Plaintiff and Class Members have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

109. The law further imposes an affirmative duty on Defendants to timely disclose the unauthorized access and theft of the PII/PHI to Representative Plaintiff and Class Members so that they could and/or still can take appropriate measures to mitigate damages, protect against adverse consequences and thwart future misuse of their PII/PHI.

110. Defendants breached their duty to notify Representative Plaintiff and Class Members of the unauthorized access by waiting months after learning of the Data Breach to notify Representative Plaintiff and Class Members. and then by failing and continuing to fail to provide Representative Plaintiff and Class Members sufficient information regarding the breach. To date, Defendants have not provided sufficient information to Representative Plaintiff and Class Members regarding the extent of the unauthorized access and continue to breach their disclosure obligations to Representative Plaintiff and Class Members.

111. Further, through their failure to provide timely and clear notification of the 2021 Data Breach to Representative Plaintiff and Class Members, Defendants prevented Representative Plaintiff and Class Members from taking meaningful, proactive steps to secure their PII/PHI, and to access their medical records and histories.

112. There is a close causal connection between Defendants' failure to implement security measures to protect the PII/PHI of Representative Plaintiff and Class Members and the harm suffered or risk of imminent harm suffered by Representative Plaintiff and Class Members. Representative Plaintiff's and Class Members' PII/PHI was accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such PII/PHI by adopting, implementing, and maintaining appropriate security measures.

113. Defendants' wrongful actions, inactions, and omissions constituted (and continue to constitute) common law negligence.

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

114. The damages Representative Plaintiff and Class Members have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendants' grossly negligent conduct.

115. Additionally, 15 U.S.C. §45 (FTC Act, Section 5) prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect PII/PHI. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

116. Defendants violated 15 U.S.C. §45 by failing to use reasonable measures to protect PII/PHI and not complying with applicable industry standards, as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of PII/PHI they obtained and stored and the foreseeable consequences of the immense damages that would result to Representative Plaintiff and Class Members.

117. Defendants' violation of 15 U.S.C. §45 constitutes negligence *per se.* Defendants also violated the HIPAA Privacy and Security rules which, likewise, constitutes negligence *per se*.

118. As a direct and proximate result of Defendants' negligence and negligence *per se*, Representative Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII/PHI is used; (iii) the compromise, publication, and/or theft of their PII/PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII/PHI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the 2021 Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from embarrassment and identity theft; (vi) lost continuity in relation to their healthcare; (vii) the continued risk to their PII/PHI, which may remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect Representative Plaintiff's and Class Members' PII/PHI in their continued possession; and (viii) future costs in terms of time, effort, and money

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

that will be expended to prevent, detect, contest, and repair the impact of the PII/PHI compromised as a result of the 2021 Data Breach for the remainder of the lives of Representative Plaintiff and Class Members.

119. As a direct and proximate result of Defendants' negligence and negligence *per se*, Representative Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

120. Additionally, as a direct and proximate result of Defendants' negligence and negligence *per se*, Representative Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their PII/PHI, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the PII/PHI in their continued possession.

SECOND CLAIM FOR RELIEF
Invasion of Privacy
(Both Classes)

121. Each and every allegation of the preceding paragraphs is incorporated in this cause of action with the same force and effect as though fully set forth herein.

122. Representative Plaintiff and Class Members had a legitimate expectation of privacy to their PII/PHI and were entitled to the protection of this information against disclosure to unauthorized third parties.

123. Defendants owed a duty to Representative Plaintiff and Class Members to keep their PII/PHI confidential.

124. Defendants failed to protect and released to unknown and unauthorized third parties the PII/PHI of Representative Plaintiff and Class Members.

125. Defendants allowed unauthorized and unknown third parties access to and examination of the PII/PHI of Representative Plaintiff and Class Members, by way of Defendants' failure to protect the PII/PHI.

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

126. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII/PHI of Representative Plaintiff and Class Members is highly offensive to a reasonable person.

127. The unauthorized intrusion was into a place or thing which was private and is entitled to be private. Representative Plaintiff and Class Members disclosed their PII/PHI to Defendants as part of obtaining services from Defendants, but privately with an intention that the PII/PHI would be kept confidential and would be protected from unauthorized disclosure. Representative Plaintiff and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

128. The 2021 Data Breach constitutes an intentional interference with Representative Plaintiff's and Class Members' interests in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

129. Defendants acted with a knowing state of mind when they permitted the 2021 Data Breach to occur because it was with actual knowledge that their information security practices were inadequate and insufficient.

130. Because Defendants acted with this knowing state of mind, they had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Representative Plaintiff and Class Members.

131. As a proximate result of the above acts and omissions of Defendants, the PII/PHI of Representative Plaintiff and Class Members was disclosed to third parties without authorization, causing Representative Plaintiff and Class Members to suffer damages.

132. Unless and until enjoined, and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Representative Plaintiff and Class Members in that the PII/PHI maintained by Defendants can be viewed, distributed, and used by unauthorized persons for years to come. Representative Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Representative Plaintiff and/or Class Members.

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

THIRD CLAIM FOR RELIEF
Breach of Confidence
(Both Classes)

133. Each and every allegation of the preceding paragraphs is incorporated in this cause of action with the same force and effect as though fully set forth herein.

134. At all times during Representative Plaintiff's and Class Members' interactions with Defendants, Defendants were fully aware of the confidential nature of the PII/PHI that Representative Plaintiff and Class Members provided to them.

135. As alleged herein and above, Defendants' relationship with Representative Plaintiff and the Classes was governed by promises and expectations that Representative Plaintiff and Class Members' PII/PHI would be collected, stored, and protected in confidence, and would not be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties.

136. Representative Plaintiff and Class Members provided their respective PII/PHI to Defendants with the explicit and implicit understandings that Defendants would protect and not permit the PII/PHI to be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties.

137. Representative Plaintiff and Class Members also provided their PII/PHI to Defendants with the explicit and implicit understandings that Defendants would take precautions to protect their PII/PHI from unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing, such as following basic principles of protecting their networks and data systems.

138. Defendants voluntarily received, in confidence, Representative Plaintiff's and Class Members' PII/PHI with the understanding that the PII/PHI would not be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by and/or viewed by the public or any unauthorized third parties.

139. Due to Defendants' failure to prevent, detect, and avoid the 2021 Data Breach from occurring by, *inter alia*, not following best information security practices to secure Representative

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

Plaintiff's and Class Members' PII/PHI, Representative Plaintiff's and Class Members' PII/PHI was accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by and/or viewed by unauthorized third parties beyond Representative Plaintiff's and Class Members' confidence, and without their express permission.

140. As a direct and proximate cause of Defendants' actions and/or omissions, Representative Plaintiff and Class Members have suffered damages as alleged herein.

141. But for Defendants' failure to maintain and protect Representative Plaintiff's and Class Members' PII/PHI in violation of the parties' understanding of confidence, their PII/PHI would not have been accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by and/or viewed by unauthorized third parties. The 2021 Data Breach was the direct and legal cause of the misuse of Representative Plaintiff's and Class Members' PII/PHI, as well as the resulting damages.

142. The injury and harm Representative Plaintiff and Class Members suffered and will continue to suffer was the reasonably foreseeable result of Defendants' unauthorized misuse of Representative Plaintiff's and Class Members' PII/PHI. Defendants knew their data systems and protocols for accepting and securing Representative Plaintiff's and Class Members' PII/PHI had security and other vulnerabilities that placed Representative Plaintiff's and Class Members' PII/PHI in jeopardy.

143. As a direct and proximate result of Defendants' breaches of confidence, Representative Plaintiff and Class Members have suffered and will suffer injury, as alleged herein, including but not limited to (a) actual identity theft; (b) the compromise, publication, and/or theft of their PII/PHI; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII/PHI; (d) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the 2021 Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (e) the continued risk to their PII/PHI, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

Class Members' PII/PHI in their continued possession; (f) future costs in terms of time, effort, and money that will be expended as result of the 2021 Data Breach for the remainder of the lives of Representative Plaintiff and Class Members; and (g) the diminished value of Representative Plaintiff's and Class Members' PII/PHI; and (h) the diminished value of Defendants' services Representative Plaintiff and Class Members paid for and received.

FOURTH CLAIM FOR RELIEF
Information Practices Act of 1977 (Cal. Civ. Code §1798, *et seq.*)
(California Subclass Only)

144. Each and every allegation of the preceding paragraphs is incorporated in this cause of action with the same force and effect as though fully set forth herein.

145. Defendants were legally obligated to "establish appropriate and reasonable administrative, technical, and physical safeguards to ensure compliance with the [Information Practices Act of 1977], to ensure the security and confidentiality of records, and to protect against anticipated threats or hazards to their security or integrity which could result in any injury." Cal. Civ. Code § 1798.21.

146. Defendants failed to establish appropriate and reasonable administrative, technical, and physical safeguards to ensure compliance with the Information Practices Act of 1977 with regard to the PII and PHI of Representative Plaintiff and members of the California Subclass.

147. Defendants failed to ensure the security and confidentiality of records containing the PII and PHI of Representative Plaintiff and members of the California Subclass.

148. Defendants failed to protect against anticipated threats and hazards to the security and integrity of records containing the PII and PHI of Representative Plaintiff and members of the California Subclass.

149. As a result of these failures, Representative Plaintiff and members of the California Subclass have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, inter alia, (i) an imminent, immediate and continuing increased risk of identity theft, identify fraud, and medical fraud - risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) breach of the

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

confidentiality of their PII/PHI, (iv) deprivation of the value of their PII/PHI, for which there is a well-established national and international market, and/or (v) the financial and temporal cost of monitoring her credit, monitoring her financial accounts and mitigating their damages.

150. Representative Plaintiff and members of the California Subclass are also entitled to injunctive relief under California Civil Code § 1798.47.

FIFTH CLAIM FOR RELIEF
Confidentiality of Medical Information Act (Cal. Civ. Code §56, *et seq.*)
(California Subclass Only)

151. Each and every allegation of the preceding paragraphs is incorporated in this cause of action with the same force and effect as though fully set forth herein.

152. Under California Civil Code §56.06, Defendants is deemed a "provider of healthcare" and is therefore subject to the CMIA, California Civil Code §§ 56.10(a), (d) (e), 56.36(b), 56.101(a) and (b).

153. Under CMIA, California Civil Code §56.05(k), Representative Plaintiff and members of the California Subclass are deemed "patients."

154. As defined in CMIA, California Civil Code §56.05(j), Defendants disclosed "medical information" to unauthorized persons without obtaining consent, in violation of §56.10(a). Defendants' misconduct, including failure to adequately detect, protect, and prevent unauthorized disclosure, directly resulted in the unauthorized disclosure of Representative Plaintiff's and members of the California Subclass' PII/PHI to unauthorized persons.

155. Defendants' misconduct, including protecting and preserving the confidential integrity of their clients'/customers' PII/PHI, resulted in unauthorized disclosure of sensitive and confidential PII that belongs to Representative Plaintiff and members of the California Subclass to unauthorized persons, breaching the confidentiality of that information, thereby violating California Civil Code §§ 56.06 and 56.101(a)..

156. Representative Plaintiff and members of the California Subclass have all been and continue to be harmed as a direct, foreseeable and proximate result of Defendants' breach because Representative Plaintiff and members of the California Subclass face, now and in the future, an

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

imminent threat of identity theft, fraud and for ransom demands. They must now spend time, effort and money to constantly monitor their accounts and credit to surveille for any fraudulent activity.

157. Representative Plaintiff and members of the California Subclass were injured and have suffered damages, as described above, from Defendants' illegal disclosure and negligent release of their PII/PHI in violation of Cal. Civ. Code §§ 56.10 and 56.101, and therefore seek relief under Civ. Code §§ 56.35 and 56.36, including actual damages, nominal statutory damages of $1,000, punitive damages of $3,000, injunctive relief, and attorney fees and costs.

SIXTH CLAIM FOR RELIEF
Breach of Implied Contract

158. Each and every allegation of the preceding paragraphs is incorporated in this cause of action with the same force and effect as though fully set forth herein.

159. Through their course of conduct, Defendants, Representative Plaintiff and Class Members entered into implied contracts for the Defendants to implement data security adequate to safeguard and protect the privacy of Representative Plaintiff's and Class Members' PII/PHI.

160. Defendants required Representative Plaintiff and Class Members to provide and entrust their PII/PHI, including full names, birthdates and prescription information and/or other information, as a condition of getting their prescriptions filled by Defendants Rite Aid and CHC and processed by Defendants CaptureRx.

161. Defendants Rite Aid and CHC solicited and invited Representative Plaintiff and Class Members to provide their PII/PHI as part of these Defendants' regular business practices. Representative Plaintiff and Class Members accepted Defendants Rite Aid's and CHC's offers and provided their PII/PHI to these Defendants.

162. As a condition of being direct customers of Defendants Rite Aid and CHC, and indirect customers of Defendants CaptureRx, Representative Plaintiff and Class Members provided and entrusted their PII/PHI to all Defendants. In so doing, Representative Plaintiff and Class Members entered into implied contracts with Defendants by which Defendants agreed to safeguard and protect such non-public information, to keep such information secure and

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

confidential, and to timely and accurately notify Representative Plaintiff and Class Members if their data had been breached and compromised or stolen.

163. A meeting of the minds occurred when Representative Plaintiff and Class Members agreed to, and did, provide their PII/PHI to Defendants, in exchange for, amongst other things, the protection of their PII/PHI.

164. Representative Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendants.

165. Defendants breached the implied contracts they made with Representative Plaintiff and Class Members by failing to safeguard and protect their PII/PHI by failing to provide timely and accurate notice to them that their PII/PHI was compromised as a result of the 2021 Data Breach.

166. As a direct and proximate result of Defendants' above-described breach of implied contract, Representative Plaintiff and Class Members have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; lost work time; and other economic and non-economic harm.

SEVENTH CLAIM FOR RELIEF
Breach of the Implied Covenant of Good Faith and Fair Dealing

167. Each and every allegation of the preceding paragraphs is incorporated in this cause of action with the same force and effect as though fully set forth herein.

168. Every contract in the State of California has an implied covenant of good faith and fair dealing. This implied covenant is an independent duty and may be breached even when there is no breach of the contract's express terms.

169. Representative Plaintiff and Class Members have complied with and performed all conditions of their contracts with Defendants, and each of them.

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

170. Defendants breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard PII/PHI, failing to timely and accurately disclose the 2021 Data Breach to Representative Plaintiff and Class Members and continued acceptance of PII/PHI and storage of other personal information after Defendants knew or should have known of the security vulnerabilities of the systems that were exploited in the 2021 Data Breach.

171. Defendants acted in bad faith and/or with malicious motive in denying Representative Plaintiff and Class Members the full benefit of their bargains as originally intended by the parties, thereby causing them injury in an amount to be determined at trial.

EIGHTH CLAIM FOR RELIEF
Unfair Business Practices
(Cal. Bus. & Prof. Code, §17200, *et seq.*)
(California Subclass Only)

172. Each and every allegation of the preceding paragraphs is incorporated in this cause of action with the same force and effect as though fully set forth herein.

173. Representative Plaintiff and members of the California Subclass further bring this cause of action, seeking equitable and statutory relief to stop the misconduct of Defendants, as complained of herein.

174. Defendants has engaged in unfair competition within the meaning of California Business & Professions Code §§17200, *et seq.*, because Defendants' conduct is unlawful, unfair and fraudulent, as herein alleged.

175. Representative Plaintiff, the members of the California Subclass, and Defendants are each a "person" or "persons" within the meaning of § 17201 of the California Unfair Competition Law ("UCL").

176. The knowing conduct of Defendants, as alleged herein, constitutes an unlawful and/or fraudulent business practice, as set forth in California Business & Professions Code §§17200-17208. Specifically, Defendants conducted business activities while failing to comply with the legal mandates cited herein, including HIPAA. Such violations include, but are not necessarily limited to:

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

a. failure to maintain adequate computer systems and data security practices to safeguard PII/PHI;

b. failure to disclose that their computer systems and data security practices were inadequate to safeguard PII/PHI from theft;

c. failure to timely and accurately disclose the 2021 Data Breach to Representative Plaintiff and members of the California Subclass;

d. continued acceptance of PII/PHI and storage of other personal information after Defendants knew or should have known of the security vulnerabilities of the systems that were exploited in the 2021 Data Breach; and

e. continued acceptance of PII/PHI and storage of other personal information after Defendants knew or should have known of the 2021 Data Breach and before they allegedly remediated the 2021 Data Breach.

177. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard the PII/PHI of Representative Plaintiff and members of the California Subclass, deter hackers, and detect a breach within a reasonable time, and that the risk of a data breach was highly likely.

178. In engaging in these unlawful business practices, Defendants have enjoyed an advantage over their competition and a resultant disadvantage to the public and members of the California Subclass.

179. Defendants' knowing failure to adopt policies in accordance with and/or adhere to these laws, all of which are binding upon and burdensome to Defendants' competitors, engenders an unfair competitive advantage for Defendants, thereby constituting an unfair business practice, as set forth in California Business & Professions Code §§17200-17208.

180. Defendants have clearly established a policy of accepting a certain amount of collateral damage, as represented by the damages to Representative Plaintiff and members of the California Subclass herein alleged, as incidental to their business operations, rather than accept the alternative costs of full compliance with fair, lawful and honest business practices ordinarily borne by responsible competitors of Defendants and as set forth in legislation and the judicial record.

181. The UCL is, by its express terms, a cumulative remedy, such that remedies under its provisions can be awarded in addition to those provided under separate statutory schemes and/or

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

common law remedies, such as those alleged in the other Counts of this Complaint. *See* Cal. Bus. & Prof. Code § 17205.

182. Representative Plaintiff and members of the California Subclass request that this Court enter such orders or judgments as may be necessary to enjoin Defendants from continuing their unfair, unlawful, and/or deceptive practices and to restore to Representative Plaintiff and members of the California Subclass any money Defendants acquired by unfair competition, including restitution and/or equitable relief, including disgorgement or ill-gotten gains, refunds of moneys, interest, reasonable attorneys' fees, and the costs of prosecuting this class action, as well as any and all other relief that may be available at law or equity.

NINTH CLAIM FOR RELIEF
Unjust Enrichment

183. Each and every allegation of the preceding paragraphs is incorporated in this cause of action with the same force and effect as though fully set forth herein.

184. By their wrongful acts and omissions described herein, Defendants has obtained a benefit by unduly taking advantage of Representative Plaintiff and Class Members.

185. Defendants, prior to and at the time Representative Plaintiff and Class Members entrusted their PII/PHI to Defendants for the purpose of obtaining health services, believing that Defendants would keep such PII/PHI secure.

186. Defendants was aware or should have been aware that reasonable patients and consumers would have wanted their PII/PHI kept secure and would not have contracted with Defendants, directly or indirectly, had they know that Defendants' information systems were sub-standard for that purpose.

187. Defendants were also aware that, if the substandard condition of and vulnerabilities in their information systems were disclosed, it would negatively affect Representative Plaintiff's and Class Members' decisions to seek health care series therefrom

188. Defendants failed to disclose facts pertaining to their substandard information systems, defects and vulnerabilities therein before Representative Plaintiff and Class Members made their decisions to make purchases, engage in commerce therewith, seek health care services

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

from information or any of them. Instead, Defendants suppressed and concealed such information. By concealing and suppressing that information, Defendants denied Representative Plaintiff and Class Members the ability to make a rational and informed purchasing and health care decisions and took undue advantage of Representative Plaintiff and Class Members.

189. Defendants was unjustly enriched at the expense of Representative Plaintiff and Class Members. Defendants received profits, benefits, and compensation, in part, at the expense of Representative Plaintiff and Class Members. By contrast, Representative Plaintiff and Class Members did not receive the benefit of their bargain because they paid for products and paid for health care services that did not satisfy the purposes for which they bought /sought them.

190. Since Defendants' profits, benefits, and other compensation were obtained by improper means, Defendants is not legally or equitably entitled to retain any of the benefits, compensation or profits they realized from these transactions.

191. Representative Plaintiff and Class Members seek an Order of this Court requiring Defendants to refund, disgorge, and pay as restitution any profits, benefits, and other compensation obtained by Defendants from their wrongful conduct and/or the establishment of a constructive trust from which Representative Plaintiff and Class Members may seek restitution.

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

PRAYER FOR RELIEF

WHEREFORE, Representative Plaintiff, on behalf of herself and each member of the proposed National Class and the California Subclass, respectfully request that the Court enter judgment in her/their favor and for the following specific relief against Defendants as follows:

1. That the Court declare, adjudge, and decree that this action is a proper class action and certify each of the proposed classes and/or any other appropriate subclasses under F.R.C.P. Rule 23 (b)(1), (b)(2), and/or (b)(3), including appointment of Representative Plaintiff's counsel as Class Counsel;

2. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

3. That the Court enjoin Defendants, and each of them, ordering them to cease and desist from unlawful activities in further violation of California Business and Professions Code §17200, *et seq.*;

4. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Representative Plaintiff's and Class Members' PII/PHI, and from refusing to issue prompt, complete any accurate disclosures to Representative Plaintiff and Class Members;

5. For injunctive relief requested by Representative Plaintiff and Class Members, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Representative Plaintiff and Class Members, including but not limited to an Order:

a. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

b. requiring Defendants to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

c. requiring Defendants to delete and purge the PII/PHI of Representative Plaintiff and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Representative Plaintiff and Class Members;

d. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Representative Plaintiff's and Class Members' PII/PHI;

e. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests and audits on Defendants' systems on a periodic basis;

f. prohibiting Defendants from maintaining Representative Plaintiff's and Class Members' PII/PHI on a cloud-based database;

g. requiring Defendants to segment data by creating firewalls and access controls so that, if one area of Defendants' networks are compromised, hackers cannot gain access to other portions of Defendants' systems;

h. requiring Defendants to conduct regular database scanning and securing checks;

i. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800

employees' respective responsibilities with handling PII/PHI, as well as protecting the PII/PHI of Representative Plaintiff and Class Members;

j. requiring Defendants to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs, and systems for protecting PII/PHI;

k. requiring Defendants to implement, maintain, review, and revise as necessary a threat management program to appropriately monitor Defendants' networks for internal and external threats, and assess whether monitoring tools are properly configured, tested, and updated;

l. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves.

6. For prejudgment interest on all amounts awarded, at the prevailing legal rate;

7. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

8. For all other Orders, findings, and determinations identified and sought in this Complaint.

JURY DEMAND

Representative Plaintiff, individually and on behalf of the Plaintiff Classes, hereby demand a trial by jury for all issues triable by jury

Dated: August 10, 2021

SCOTT COLE & ASSOCIATES, APC

By: _____
Scott Edward Cole, Esq.
Attorneys for Representative Plaintiff
and the Plaintiff Classes

SCOTT COLE & ASSOCIATES, APC
ATTORNEYS AT LAW
555 12TH STREET, SUITE 1725
OAKLAND, CA 94607
TEL: (510) 891-9800